Amendments to the Claims:

The Listing of Claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently amended)A method for managing a security policy for one or more users in a network, comprising:

a) running a policy management program on a computer in communication with the network;

b) enabling creation of a security policy document in a portable representation language using the policy management program, including selection and inclusion in the security policy document of a plurality of data elements for communicating the security policy to the one or more users and of at least one data element for implementing the security policy on computer systems in the network;

c) enabling the one or more users on the network to view the security policy document using the plurality of data elements for communicating the security policy to the one or more users included in the security policy document; and

d) receiving electronic data relevant to user viewing of the security policy document using the policy management program.

2. (Original) The method of claim 1, further comprising verifying a degree of user compliance with the security policy by using the policy management program to assess the received data.

3. (Original) The method of claim 2, wherein the received data includes a timestamp denoting the time a user acknowledges viewing of the security policy document.

4. (Original) The method of claim 2, wherein the received data includes quiz results indicative of the user comprehension of the viewed security policy document.

5. (Original) The method of claim 1, wherein enabling the creation of the security policy document comprises enabling selection of security policies from a set of options.

6. (Original) The method of claim 5, wherein the security policies selected from the set of options reside in a library in communication with the policy management program.

7. (Original) The method of claim 1, wherein enabling the users on the network to view the security policy document comprises enabling pre-selection of a group of users to view the security policy document.

8. (Original) The method of claim 1, further comprising electronically providing a quiz to assess user comprehension of the viewed security policy document.

9. (Original) The method of claim 1, wherein enabling the creation of the security policy document further comprises enabling creation of a quiz associated with the security policy document.

10. (Original) The method of claim 8, wherein the received data includes user responses to the quiz.

11. (Original) A method for managing a security policy for one or more first computers in a network, comprising:

a) running a software program on a second computer in communication with the network;

b) enabling creation of a security policy document using the software program by enabling selection of security policies from a set of options; and

c) automatically configuring the security policy document to provide one or more technical controls for implementing the security policy on at least one first computer.

12. (Original) The method of claim 11, wherein the security policies selected from the set of options reside in a library in communication with the software program.

13. (Original) The method of claim 11, wherein two of the first computers operate in accordance with different operating systems.

14. (Original) The method of claim 11, wherein the technical controls comprise a format interpretable by at least one first computer.

15. (Original) The method of claim 11, wherein the security policy document is represented by a markup language.

16. (Original) The method of claim 11, further comprising distributing detect rules to at least one first computer.

17. (Original) The method of claim 16, further comprising electronically notifying an administrator when at least one first computer is out of compliance.

18. (Original) The method of claim 11, further comprising distributing the one or more technical controls to at least one first computer.

19. (Original) The method of claim 18, further comprising running a second software program on at least one first computer to allow at least one first computer to interpret the distributed technical controls.

20. (Original) The method of claim 19, wherein the second software program

uses metacommands to convert the technical controls into instructions interpretable by an operating system running on at least one first computer.

21. (Original) The method of claim 11, further comprising receiving data relevant to compliance of at least one first computer with the one or more technical controls using the software program.

22. (Original) The method of claim 21, further comprising assessing the received data using a third software program.

23. (Original) The method of claim 22, wherein the third software program comprises a security management program.

24. (Original) The method of claim 21, further comprising verifying a degree of compliance of at least one first computer with the one or more technical controls by using the software program to assess the received data.

25. (Original) The method of claim 24, wherein the received data comprises compliance score data.

26. (Original) A method for managing a security policy for one or more users and one or more first computers in a network, comprising:

a) running a software program on a second computer in communication with the network;

b) creating a security policy document using the software program; and

c) automatically configuring the security policy document to create (i) a human-readable security policy document, and (ii) a machine-readable security policy document containing technical controls readable by at least one first computer.

27. (Original) The method of claim 26, further comprising allowing the users to view the human-readable security policy document via the network.

28. (Original) The method of claim 27, wherein allowing the users to view the human-readable security policy document comprises pre-selecting a group of users to view the security policy document.

29. (Original) The method of claim 27, further comprising electronically receiving data relevant to user viewing of the security policy document.

30. (Original) The method of claim 29, wherein the received data includes a timestamp denoting the time a user acknowledged viewing the security policy.

31. (Original) The method of claim 29, further comprising verifying a degree of user compliance with the security policy by using the software program to assess the received data.

32. (Original) The method of claim 31, wherein the received data includes quiz results indicative of the user comprehension of the viewed security policy document.

33. (Original) The method of claim 26, wherein creating the security policy document comprises selecting security policies from a set of options.

34. (Original) The method of claim 33, wherein the security policies selected from the set of options reside in a library in communication with the software program.

35. (Original) The method of claim 26, wherein the human-readable security policy document includes a quiz to test user comprehension of the security policy

document.

36. (Original) The method of claim 26, further comprising electronically providing a quiz to assess user comprehension of the viewed security policy document.

37. (Original) The method of claim 26, wherein enabling the creation of the security policy document further comprises enabling creation of a quiz associated with the security policy document.

38. (Original) The method of claim 26, further comprising distributing the machine-readable security policy document to at least one first computer to implement the security technical controls thereon.

39. (Original) The method of claim 38, further comprising running a second software program on at least one first computer to allow at least one first computer to interpret the distributed technical controls.

40. (Original) The method of claim 39, wherein the second software program uses metacommands to convert the technical controls into instructions interpretable by an operating system running on at least one first computer.

41. (Original) The method of claim 38, further comprising receiving data relevant to compliance of at least one first computer with the technical controls using the software program.

42. (Original) The method of claim 41, further comprising assessing the received data using a third software program.

43. (Original) The method of claim 42, wherein the third software program

comprises a security management program.

44. (Original) The method of claim 41, further comprising verifying a degree of compliance of at least one first computer with the technical controls by using the software program to assess the received data.

45. (Original) The method of claim 44, wherein the received data comprises compliance score data.

46. (Original) The method of claim 26, wherein two of the first computers operate in accordance with different operating systems.

47. (Original) The method of claim 26, wherein the technical controls comprise a format interpretable by at least one first computer.

48. (Original) The method of claim 47, wherein the security policy documents is represented by a markup language.

49. (Original) The method of claim 26, further comprising distributing detect rules to at least one first computer.

50. (Original) The method of claim 49, further comprising electronically notifying an administrator when at least one first computer is out of compliance.

51. (Original) A system for managing a security policy for one or more users and for one or more first computers in a network, comprising:

a) a first device containing a first program for creating a security policy document in both human-readable and machine-readable formats; and

b) a second device in communication with the first device and containing a

second program for monitoring the security compliance of at least one first computer; wherein at least one first computer contains a third program for receiving the machine-readable format of the security policy document.

52. (New) The method of claim 1, wherein the portable representation language comprises a structured data representation language.

53. (New) The method of claim 52, wherein the plurality of data elements for communicating the security policy to the one or more users include a policy statement element, a policy commentary element and an example element and wherein the at least one data element for implementing the security policy on computer systems in the network includes a platform control element specific to a platform type corresponding to an operating system of ones of the computer systems.

54. (New) The method of claim 1, wherein enabling creation of the security policy document comprises enabling creation of a plurality of security policy documents associated with the security policy, ones of the security policy documents including data elements for different platform types corresponding to operating systems of the computer systems in the network.

55. (New) The method of claim 11, wherein the one or more first computers in the network comprises a plurality of first computers, ones of which are different platform types corresponding to operating systems of the respective first computers, the method further comprising automatically configuring the security policy document to include a plurality of platform controls, ones of which include commands for enforcing the security policy on the different platform types corresponding to operating systems of the plurality of first computers in the network.

56. (New) The method of claim 11, wherein the one or more first computers

in the network comprises a plurality of first computers, ones of which are different platform types corresponding to operating systems of the respective first computers and wherein enabling creation of a security policy document comprises enabling creation of a plurality of security policy documents associated with the security policy, the method further comprising automatically configuring respective ones of the security policy documents to include a platform control that includes commands for enforcing the security policy on a corresponding one of the different platform types.